THE SOCIAL, LEGAL, TECHNICAL PERSPECTIVE OF CYBERSTALKING IN INDIA

Ameema Miftha, Marc Conrad and Marcia Gibson
Institute for Research in Applicable Computing, University of Bedfordshire, UK

ABSTRACT

This paper explores the social, technical and legal perspectives of cyberstalking in India. With the growth of the Internet, cyberstalking as a potential cybercrime has achieved many fold growths in India over the last decade. Factors such as, poor social perception towards the crime, cultural conflict and ignorance, subjective characteristics and habits of the victims, freedom and remoteness of Internet technologies and inadequacy of cyber legislation in preventing and penalising the crime have facilitated the rapid growth and proliferation of cyberstalking in India. In addition to low levels of awareness on the part of the victim and law enforcement authorities, anecdotal evidence suggests there is a fear of secondary victimisation, both in victims and their relatives. This has become a major cause for the majority of stalking crimes to remain unregistered. In case of India, there is clear dearth of research in relation to the social, legal and technical perspectives of cyberstalking. None of the Indian studies have provided conclusive findings on these three perspectives. This paper recommends further comprehensive studies into cyberstalking in India.

KEYWORDS

Cyberstalking, India, Cybercrime, Social, Culture, Legal, Technical, Perspective

1. INTRODUCTION

The rapid proliferation and global integration of the Internet has provided both virtue and vice. On one hand, Internet driven information and communication technologies (ICT) have revolutionised communication, offering speed and convenience. On the other, it has facilitated cyberstalking as a prominent cybercrime (Madhavi & Prasad, 2014; Drebing et al, 2014). Cyberstalking refers to the repeated pursuit of an individual using electronic or Internet-capable devices (Drebing et al, 2014). It includes a range of unwanted behaviours such as, “name-calling, trolling, doxing, open and escalating threats, vicious sexist, racist, and homophobic rants, attempts to shame others, and, direct efforts to embarrass or humiliate people” (cited in Zarina et al, 2016).

Though as a technology enabled crime, cyberstalking has become a global phenomenon, in the Indian scenario it has received limited attention both in academic and social research fields. However, as per the available statistics, from developed countries such as the USA and UK, cybercrimes in India have achieved manifold growths over the last decade (Sadotra and Kour, 2016). The National Crime Records Bureau (NCRB) estimates the cyber victimisation of 100,000 persons a day. They report an increase of 2,400**%** in cybercrimes over the last decade .cybercrime registered cases in India have increased from 9,622 in 2014 to 11,592 in 2015 with nearly one-third of the crimes committed for financial gain. The number of individuals arrested for cybercrime increased by over 41% during the same period (NCRB, 2015).

In this paper we explore the social, technical and legal perspectives of cyberstalking in India.

ISBN: 978-989-8533-60-9 © 2017

2. SOCIAL PERSPECTIVE

From the social perspective, despite global and national reporting on the severity of cyberstalking consequences (Uptoti,2014; Drebing et al, 2014; Saridakis, et al, 2016), the level of cyberstalking awareness remains low (Kashmiria, 2014). General social ignorance and cultural conflict in part of the victims and their relatives regarding the possibility of extreme consequences pertaining to physical harm, suicide and murder threats contributes towards the perceptual ignorance (Roy, 2015; Sadotra and Kour, 2015). As a result, the majority of cyberstalking incidents go unpunished and unregistered in India (Roy, 2015).

The available other country specific research works do not directly address the role of socio-cultural influences in shaping the perceptions of the victims towards cyberstalking, they view cyberstalking from perspectives of the victims' personal habits, characteristics and life styles (Zarina et al, 2016; Saridakis et al, 2016). For example, Zarina et al, (2016) in their research article explained the proliferation of the cyberstalking phenomena with the Routine Activity Theory (RAT) and Life Style Exposure theory from the victims' perspectives. They found inconsistent empirical evidence in support of their explanation. Their findings suggest that, the extensions of those theories partially explain the victims' roles in facilitating the crime. Similarly, Saridakis et al (2016) also view that from the perspective of the RAT, the victim's regular and habitual activities provide opportunities for the stalker to be engaged in cyberstalking. Their findings observe a statistically dominant association between Social Networking Service (SNS) users and victimisation. Their findings also suggest that SNS users with high awareness of privacy and controlling of information are less likely to become victimised. The findings of the above mentioned studies may provide useful insights (particularly in the context of India) as the victims' personal habits and lifestyles are often influenced by their prevailing socio-cultural set.

Cyberstalking is a continuous, repeated and persistent activity of the stalker to disturb, harm and control the victim. The harmful message transits from the virtual world to the psychological and physical world of the victim on a continuous basis and ultimately puts the victim in severe distress (Frommholz et al, 2016). If the process of stalking activities are not stopped 'in time', it can result in severe consequences such as suicide, murder, depression and other severe incidences like rape and acid attacks. Here, a longer process time and transit time gap might influence the severity. The empirical and literature works in relation to the role of the process time and the victim's perceptual transit time span from virtual world to the resulting consequences in the physical world remain limited. Cyberstalking takes place over multiple related incidents. Persistent delay in blocking the stalker's activities through legal or technological means can put the victim in severe distress and in extreme cases lead to physical injury or death. Similarly, quick reactions on the part of the victim (i.e. to block, report or similar) can prevent such outcomes and can result in punishment of the stalker.

3. LEGAL PERSPECTIVE

From the legal perspective, unlike the countries like the US, UK, Canada and Australia which have penal provisions for criminalising cyberstalking (Joshi, 2013), the legal enforcement realisation of cyberstalking crime came very late in India. Though stalking incidents in India were reported two decades ago, the cybercrime related law came in to existence with the establishment of the IT Act, 2000 which was amended in 2008 (Sadotra and Kour, 2015). The IT Act is considered inadequate and it does not deal directly with cyberstalking as it states, "intrusion on to the privacy of individual". After some disturbing and widely reported incidents such as the December 2012 'Delhi gang rape and murder' (Joshi, 2013) and the 2013 cybercrime related incident at the Delhi Metro station (Kashmiria, 2013), women's safety has become a primary concern for law makers in India. Following these, the first legislation criminalising cyberstalking came into force in 2013 which added S.354D to the Indian Penal Code to define and punish the act of stalking (Sadotra and Kour, 2015). This law describes punishment of a minimum one year imprisonment with an extension limit up to 3 years and a fine. However, this law is considered inadequate in preventing the crime pertaining to certain acute concerns such as, poor perception in part of the victims and enforcement authorities; fear of secondary victimisation in part of the victims and the limitations of the existing enforcement law in relation to the difference in geographical jurisdictions between the place of the victim and that of the criminal (Halder & Jaishankar, 2011; Joshi, 2013; Roy, 2015).

Very few Indian perspective studies have discussed the legal enforcement status of cyberstalking in India. For example, Kashmiria (2014), views the emergence of the Internet as the opportunity and enabler for cybercrimes. By comparing the Indian cyberstalking enforcement legislation with UK and USA legislation, she finds inadequacy of the Indian cyberstalking laws in preventing the crime and punishing the criminals. Similarly, another comparative study by Halder & Jaishankar (2011) on India, UK and USA cyberstalking legislation has highlighted the importance of secondary victimisation and denial of justice as the main reasons for the proliferation of the crime. Sadotra and Kour's (2015) study demonstrates the various ways current legislation and the common law can be used to deal with cyberstalking and harassment in India. However, none of the studies have addressed the prevailing perceptual gaps on the part of the enforcement authorities and victims regarding the degree of the criminality of the cyberstalking offence.

4. TECHNICAL PERSPECTIVE

Technology plays the dual role as the facilitator and preventer of cyberstalking behaviours. The problem is how to prevent the crime by blocking the stalker's activities; and how to assist the enforcing authority in locating and identifying the stalker. The finding of a handful of HCI perspective studies suggest the factors such as ICT, internet technology and IP connected devices such as computer, smart phones and tablets coupled with communication applications such as IM and SMS together have facilitated the growth in proliferation of cyberstalking crimes (Madhavi & Prasad, 2014; Frommholz et al, 2016). These studies have also suggested the technological measures for preventing the crime and assisting the victim and the enforcing authorities in identifying and locating the stalkers Unlike face-to-face communications, text-based technology mediated communications such as email and instant messaging lack visual cues (e.g.facial expressions, body language), thereby increasing the likelihood of miscommunication which may in itself, lead to escalated conflict (Herring, S., 2003, p.612). The internet and in particular, Web also allow for the target to be researched. The resulting information may be correct or incorrect and may be taken out of the original context – again leading to an increased possibility of conflict and cyberstalking crimes.

5. DISCUSSION

The exploration of the cyberstalking phenomenon in India reveals the prevailing gaps in the socio-cultural, legal and technical parameters, leading to the following research questions and objectives.

Q1. What is the role of socio-cultural influence in shaping the perception of Indian victims towards cyberstalking?

Q2. What is the impact of process time and transit time gap of the message flow from the Indian victims 'cyber space to the psychological and physical world on the severity of the consequences?

Q3. How do Indian law enforcement authorities perceive cyberstalking as a crime?

Q4. What is the role of technology in enabling and preventing the crime?

6. CONCLUSION

With the growth of internet usage, cyberstalking as a potential cybercrime has achieved many fold growths in India over the last decade. Factors such as, poor social perception and awareness towards the crime, cultural conflict and ignorance, subjective characteristics and habits of the victims, freedom and remoteness of the technology and inadequacy of cyber legislations in preventing and penalising the crime have facilitated the rapid growth and proliferation of cyberstalking in India. In addition, the fear of secondary victimisation on the part of the victims and their relatives has become the major cause for the majority of the stalking crimes remain unregistered. In case of India, there is a clear dearth of research in relation to the social, legal and technical perspectives of cyberstalking. None of the Indian studies provide conclusive findings and we encourage the research community to address this with future research.

REFERENCES

Drebing, H, Bailer J., Anders, A., Wagner H., and Gallas, C. (2014), *Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact upon Victims,* Cyberpsychology, Behaviour, and Social Networking, Volume 17

Frommholz, I., Khateeb, H.M., Martin Potthast, M., Ghasem, Z.,Shukla, M.,Short, E (2016), *On Textual Analysis and Machine Learning for Cyber stalking Detection,* The National Centre for Cyberstalking Research

George Saridakis, G., Benson, V., Ezingeard, J. N., Tennakoon, H. (2016), *Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users*, Technological Forecasting & Social Change 102 (2016) 320–330

Halder, D. and Jaishankar, K., (2011), *Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India, Victims and Offenders*, 6:386–398,

Herring, Susan. 2003. *Computer-mediated discourse*. In Deborah Schiffrin, Deborah Tannen and Heidi E. Hamilton (eds.), 612634. The handbook of discourse analysis. Oxford: Blackwell.

Joshi, D., (2013), *India's Criminal Law Amendment to Include Cyber Stalking, Harassment and Voyeurism,* Centre for Internet and Society,

Kashmiria, S., (2014), *Mapping Cyber Crimes against Women in India,* International Research Journal of Commerce and Law (IRJCL) Volume -1, Issue -5, Available:

Madhavi, V. S. (2014), *Dynamic Encryption Driven over Secure IM System*, International Journal of Advanced Research in Computer Science and Software Engineering 4(2), February - 2014, pp. 622-627,

National Crime Research Bureau (NCRB) Report, 2015, Online Harassment/Cyberstalking Statistics, Available: http://www.business-standard.com/article/current-affairs/indian-cyber-crime-soars-350-in-3-years-115011900329_1.html

Roy, P.K., (2015), *why online harassment goes unpunished in India,*

Sadotra, P and Kour,J.,(2015), *The Technical and Legal Perspective of Cyber Stalking*, International journal of research pedagogy and technology in education and movement sciences (items) vol. 03, issue. 03

Zarina, V.I., Danielle M. Reynald, D.M and Michael Townsley, M., (2016), *Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization*, Journal of Contemporary Criminal Justice, Vol. 32(2) 169–188 SAGE